UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/217,932	12/22/1998	EN-SEUNG KANG	P55501	3765

7590 04/08/2004

ROBERT E BUSHNELL
1522 K STREET, N.W.
SUITE 300
WASHINGTON, DC 20005-1245

EXAMINER	
ZAND, KAMBIZ	
ART UNIT	**PAPER NUMBER**
2132	21

DATE MAILED: 04/08/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/217,932	KANG ET AL.	
	Examiner	Art Unit	
	Kambiz Zand	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 January 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *20-33,70-88 and 95-98* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *95-98* is/are allowed.

6)☒ Claim(s) *20-31,33,70-73,75-80,82 and 85-88* is/are rejected.

7)☒ Claim(s) *32,74,81,83 and 84* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The text of those sections of Title 35,U.S.Code not included in this section can be found in the prior office action.
2. The prior office actions are incorporated herein by reference. In particular, the observations with respect to claim language, and response to previously presented arguments.
3. Claims 89-94 have been canceled.
4. Claims 20-33, 28-33, 70-72, 74, 79-85 and 87 have been amended.
5. New claims 95-98 have been added.
6. Claims 20-33, 70-88 and 95-98 are pending.
7. Examiner withdraws objection to the specification due to clarification by the applicant.
8. Examiner withdraws rejection of the claims 70-94 under 35 U.S.C 112-second paragraphs due to clarification and correction by the applicant.

Response to Arguments

9. Applicant's arguments filed 01/27/04 have been fully considered; and based on the Applicant's persuasive arguments, the rejection of claims 74, 81, 83-84 and 95-98 have been withdrawn . However Applicant's arguments with respect to the other pending claims are moot in view of new ground(s) of rejection.

As per Applicant's argument with respect to claim 20, 23, 25, 28, 30 and 31, Examiner refers Applicant to col.6, lines 29-34 of Pinder where the CW key is randomly being generated and lines 35-46 where this random key generator is generated according to the receiving set top box where the information authorization are stored such as a key for service, subscriber identity that is entitle to watch a program and if such subscriber is authorized then based on that identity the random generated key being generated and based on that additional factor the decryption is being done.

The example given by applicant that identity of a user should be something like social security number or driver license number and that the identity should not be "limited to a particular playback apparatus" and "serial number of DHCT333 is not equivalent to identity character of a user" on page 25 of the response are not persuasive. Examiner considers any numbers or characters that identify an entity such as a user as an identity character. As an example plate number of a car, not only identify the character of a car, but it also identify the owner of the car. Examiner suggests considering confidential identity character such as social security number or password, then the claim language should specify such uniqueness in a clear and concise manner.

Claim Rejections - 35 USC § 112

10. **Claim 23-24** are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

11. **Claim 23-24** recites the limitation "the user" in line 17 of the claim 23. There is insufficient antecedent basis for this limitation in the claim. It is not clear if "the user is authorized" is the same user that its identity character transmitted to said server location or another entity. Appropriate correction or clarification is requested.

Claim Rejections - 35 USC § 103

12. **Claims 20-27, 29, 70-71, 73-80, 82 and 85-88** are rejected under 35 U.S.C. 103(a) as being unpatentable over Pinder et al (6,105,134 A) cited in the PTO 892, paper number 9 in view of Weber (5,812,668 A).

As per claims 20, 21, 70 and 79 Pinder et al (6,105,134 A) teach a digital content encryption and decryption apparatus of a digital content transmission system protocol, digital content encryption apparatus, method of the digital content transmission system (see abstract) comprising: a protocol format generator (see fig.6; col.4, lines 1-26), said protocol format generator generating a copyright protection protocol in response to identity characters of a user (see col.12, lines 47-58), said copyright protection protocol

including a header (see fig.6 and 10) and digital contents (see fig.10), said digital contents being encrypted (see fig.2A; and 3), said header having information for decrypting and explaining the digital contents (see fig.11 and 21; col.20, lines 66-67 and col.21, lines 1-13); and a protocol format decoder located at said terminal unit, said protocol format decoder having decryption algorithm (see fig.1;2B; col.4, lines 45-48), using key information said protocol format decoder decrypting (see col. 4, lines 45-48; col.15, lines 55-63) and replaying the digital contents according to the information of the header received from the protocol format generator (see abstract; col.7 , lines 26-65) but do not disclose that the communication is from a user to a server where the server respond to the user after receiving the user's id by providing keys for decryption of the content encrypted data. However Weber disclose the communication is from a user to a server where the server respond to the user after receiving the user's id by providing keys for decryption of the content encrypted data (see abstract; fig.2-4,6a-b; 8-10, 12a-b and 14 where the communication between the user and the server and request and challenge are clearly illustrated. It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Weber's request and challenge communication between a user and a server in Pinder's conditional access system in order to have an access to programs, digital contents based on secure identity verification and key exchange.

As per claims 22, 24 and 71 Pinder et al (6,105,134 A) teach the apparatus, method of claims 20, 23 and 70 wherein the protocol format decoder generates a user key by

adding key information to a key generation algorithm and decrypts a temporary validation key by using the user key, said protocol format decoder decrypting the encrypted digital contents with the temporary validation key, transmitted within said copyright protection protocol, said key information being formed to correspond to identity characters of a user (see col.6, lines 29-63 and col.20, lines 28-43).

As per claim 23 Pinder et al (6,105,134 A) teach a protocol, digital content encryption apparatus, method of the digital content transmission system (see abstract) comprising: a protocol format generator (see fig.6; col.4, lines 1-26), said protocol format generator generating a copyright protection protocol in response to identity characters of a user transmitted (see col.12, lines 47-58), said copyright protection protocol including a header (see fig.6 and 10) and digital contents (see fig.10), said digital contents being encrypted (see fig.2A; and 3), said header having information for decrypting and explaining the digital contents (see fig.11 and 21; col.20, lines 66-67 and col.21, lines 1-13); and a protocol format decoder located at said terminal unit, said protocol format decoder having decryption algorithm (see fig.1;2B; col.4, lines 45-48), using key information said protocol format decoder decrypting (see col. 4, lines 45-48; col.15, lines 55-63) and replaying the digital contents according to the information of the header received from the protocol format generator (see abstract; col.7 , lines 26-65). Pinder et al (6,105,134 A) further teach a temporary validation key in the form of control word that is generated randomly (see col.6, lines 29-35 and col.20, lines 28-43) and using the second key for decrypting the temporary key to decrypt the content for replay (see col.6,

lines 35-63 and col.20, lines 28-43) but do not disclose that the communication is from a user to a server where the server respond to the user after receiving the user's id by providing keys for decryption of the content encrypted data. However Weber disclose the communication is from a user to a server where the server respond to the user after receiving the user's id by providing keys for decryption of the content encrypted data (see abstract; fig.2-4,6a-b; 8-10, 12a-b and 14 where the communication between the user and the server and request and challenge are clearly illustrated. It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Weber's request and challenge communication between a user and a server in Pinder's conditional access system in order to have an access to programs, digital contents based on secure identity verification and key exchange.

As per claim 25 Pinder et al (6,105,134 A) teach a copyright protection protocol for protecting copyright of digital content (see abstract where by reassignment of keys in different times, the piracy concerns are minimized; col.1, lines 41-45), said protocol including a header (see fig.6 disclosing the delivery system; fig.10, item 1003, 1005, 1009 that disclose a header of a transport packets) and the digital contents (see fig.10, item 703 that disclose the payload that is digital contents), said digital contents being encrypted (see fig.2a and 3 that disclose encryption of the digital content by utilizing a key or DES encryption method; abstract; col.4, lines 21-31 where programs or instances are encrypted) , said header including key data for decrypting the digital contents (see fig.21 where header includes key for decryption such as item 2105, 2111,2113 and

finally 2123 where the 3-DES fpm key were used to decrypt the 2113 item to unencrypted 2123 item; col.4, lines 21-31 where the entitlement control messages contains information needed to decrypt the encrypted instances or programs that are digital content and col.20, lines 66-67 and col.21, lines 1-13), said key data being randomly generated in response to identity characters of a user (see col.6, lines 29-34 where the CW key is randomly being generated and lines 35-46 where this random key generator is generated according to the receiving set top box (the identity of the user)) transmitted to a host server from a terminal unit, wherein said terminal unit receives said protocol from said host server and replays said digital contents by decrypting the encrypted digital contents in response to the key data (see abstract; col.4 , lines 37-67) but do not disclose that the communication is from a user to a server where the server respond to the user after receiving the user's id by providing keys for decryption of the content encrypted data. However Weber disclose the communication is from a user to a server where the server respond to the user after receiving the user's id by providing keys for decryption of the content encrypted data (see abstract; fig.2-4,6a-b; 8-10, 12a-b and 14 where the communication between the user and the server and request and challenge are clearly illustrated. It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Weber's request and challenge communication between a user and a server in Pinder's conditional access system in order to have an access to programs, digital contents based on secure identity verification and key exchange.

As per claim 26 Pinder et al (6,105,134 A) teach the protocol of claim 25, further comprising a field for indicating the size of the encrypted digital contents, and an additional information field (see fig.15-17 and fig.19).

As per claims 27 and 29 Pinder et al (6,105,134 A) teach the protocol of claim 25, wherein the header comprises a copyright support field for indicating whether the digital contents are under copyright protection, an unencrypted header field, and an encrypted header field a digital content conversion format field, a key generation algorithm field, a digital content encryption algorithm field, a field for indicating user authorization information at PC, and a field for indicating user authorization information at a replaying device (see fig.19, item 1921; fig.16-19) and wherein field for number of user sharing a device is also included (see col.4, lines 37-42 wherein the number of top boxes are connected to a set of TV and wherein in col.4, lines 13-67 and col.5, lines 1-10 details all other fields that carry information between receiver and the server or provider; fig.16-19).

As per claims 72-73, 75, 77-78 and 80, 82, 85-88 Pinder et al (6,105,134 A) teach calculating a hash value by adding the user key to hash algorithm, said header including user authorization information with the hash value (see col.7, lines 66-67 and col.8, lines 1-65). Also Pinder et al (6,105,134 A) teach a protocol, digital content encryption apparatus, method of the digital content transmission system (see abstract) comprising: a protocol format generator located at a server location (see fig.6; col.4, lines 1-26), said

protocol format generator generating a copyright protection protocol in response to identity characters of a user transmitted to said server location from a terminal unit (see col.12, lines 47-58), said copyright protection protocol including a header (see fig.6 and 10) and digital contents (see fig.10), said digital contents being encrypted (see fig.2A; and 3), said header having information for decrypting and explaining the digital contents (see fig.11 and 21; col.20, lines 66-67 and col.21, lines 1-13); and a protocol format decoder located at said terminal unit, said protocol format decoder having decryption algorithm (see fig.1;2B; col.4, lines 45-48), using key information said protocol format decoder decrypting (see col. 4, lines 45-48; col.15, lines 55-63) and replaying the digital contents according to the information of the header received from the protocol format generator (see abstract; col.7 , lines 26-65). Pinder et al (6,105,134 A) further teach a temporary validation key in the form of control word that is generated randomly (see col.6, lines 29-35 and col.20, lines 28-43) and using the second key for decrypting the temporary key to decrypt the content for replay (see col.6, lines 35-63 and col.20, lines28-43).; and the header comprises a copyright support field for indicating whether the digital contents are under copyright protection, an unencrypted header field, and an encrypted header field a digital content conversion format field, a key generation algorithm field, a digital content encryption algorithm field, a field for indicating user authorization information at PC, and a field for indicating user authorization information at a replaying device (see fig.19, item 1921; fig.16-19) and wherein field for number of user sharing a device is also included (see col.4, lines 37-42 wherein the number of top boxes are connected to a set of TV and wherein in col.4, lines 13-67 and col.5, lines 1-

10 details all other fields that carry information between receiver and the server or provider; fig.16-19); and wherein the protocol format decoder generates a user key by adding key information to a key generation algorithm and decrypts a temporary validation key by using the user key, said protocol format decoder decrypting the encrypted digital contents with the temporary validation key, transmitted within said copyright protection protocol, said key information being formed to correspond to identity characters of a user (see col.6, lines 29-63 and col.20, lines 28-43).

As per claim 76 Pinder et al (6,105,134 A) teach network environment (see fig.1-4 and 5).

13. **Claims 28 and 30-31** are rejected under 35 U.S.C. 103(a) as being unpatentable over Pinder et al (6,105,134 A) in view of Weber, and further in view of Ginter et al (5,910,987A).

As per claims 28 and 30-31 Pinder et al (6,105,134 A) in view of Weber teach all limitation of the claim but do not disclose explicitly, a field for indicating the size of the unencrypted header field, an encrypted header field, a field for indicating the size of the encrypted header field and field showing the number of users. However Ginter et al (5,910,987A) teach a field for indicating the size of the unencrypted header field (see col.135, lines 29-32; fig.22 and col.154, lines 3-5), a field for indicating the size of the encrypted header field (see col.135, lines 29-32; fig.22 and col. 154, lines 3-5) and a field showing the number of users (see col. 135, lines 17-22; col.156, lines 46-55). It

would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Ginter et al (5,910,987A) in Pinder et al (6,105,134 A)'s header field's method in view of Weber in order to have a secure transaction management and electronic rights protection.

Allowable Subject Matter

14. Claims 95-98 are allowed.

An Examiner reasons for allowance will be provided upon final allowability of the application.

15. Dependent claims 96-98 are allowable as being dependent upon Independent claim 95 and having additional allowable features therein.

16. Claims 32, 74, 81, 83 and 84 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

17. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

18. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kambiz Zand whose telephone number is (703) 306-4169. The examiner can normally reached on Monday-Thursday (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone numbers for the organization where this application or proceeding is assigned as (703) 872-9306. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see

http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Kambiz Zand

04/02/04

ALBERT DECADY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100